

ABSTRACT OF THE DISCLOSURE

5 A communication system including a transmitter, a receiver, a communication link (for example, a TMDS-like link), and preferably also an external agent with which the transmitter and receiver can communicate, in which video data (or other data) are encrypted, the encrypted data are transmitted from the transmitter to the receiver, and the transmitted data are decrypted in the receiver, a transmitter and a receiver for use in such a system, a cipher engine for use in such a transmitter or receiver, a method for operating such a transmitter or receiver to encrypt or decrypt data, and a method for distributing keys to the transmitter and receiver. The receiver can be a player coupled to a downstream receiver by a TMDS-like link, and configured to re-encrypt the decrypted data (for example, using an AES or HDCP protocol) and send re-encrypted data over the link to the receiver. Optionally, the player is a repeater which translates the decrypted data from the transmitter, and then re-encrypts the translated data for transmission to the downstream receiver. The transmitter can itself be a player that receives and decrypts encrypted data from an upstream source. In preferred embodiments, the system implements a content protection protocol including a challenge-response procedure. After a new key is supplied to the receiver (and the same new key should have been supplied to the transmitter) and before the receiver can use the new key, the challenge-response procedure requires that the receiver validate the transmitter by verifying that the transmitter has proper knowledge of the new key.

10

15

20